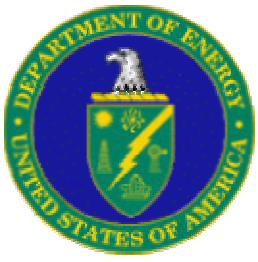
Guidance for Safety Aspects of Proposed Hydrogen Projects

August 2004



U.S. Department of Energy
Hydrogen, Fuel Cells & Infrastructure Technologies Program

Table of Contents

Guidance for Safety Aspects of Proposed Hydrogen Projects

1. Overview

This guidance document provides applicants with clarification on safety requirements for hydrogen-related solicitations from the U. S. Department of Energy (DOE) Hydrogen, Fuel Cells and Infrastructure Technologies Program. **All proposals for hydrogen-related solicitations must include a preliminary safety plan or summary (see page 2), and all funded projects must complete a more detailed safety plan before experiments and operations commence and must keep that plan current as part of the project.**

This document explains the objectives that must be met and provides examples, but it does not outline the detailed steps that must be completed in a safety plan. The responsibility of selecting and using a specific safety methodology falls upon the applicant or principal investigator and collaborating research groups. A variety of practices exist for the identification and analysis of safety hazards, and the applicants can choose an approach that is best for their project.

Safe practices in the production, storage, distribution, and use of hydrogen are essential for insurability and for the widespread acceptance of hydrogen technologies. A catastrophic failure in any hydrogen project could damage the public's perception of hydrogen and fuel cells and could also decrease the ability of hydrogen technologies to gain the approval of the insurance community, a necessary occurrence for commercialization. The DOE Hydrogen, Fuel Cells and Infrastructure Technologies Program provides for practices and awareness that will result in an environment where safety is an integral component of all of its funded projects.

A safety plan identifies immediate (primary) failure modes as well as any secondary failure modes that may come about as a result of other failures. In such a plan, every conceivable failure is identified, from catastrophic failures to benign collateral failures. Identification and discussion of perceived benign failures may lead to the identification of more serious failures.

All potential hazards in a hydrogen production, delivery, utilization, or storage system must be identified and analyzed, as well as any system aspects that may be adversely affected by a failure. These aspects include threats or impacts to:

- **Personnel.** Any hazards that pose a risk of injury or loss of life to personnel and the public at-large must be identified and eliminated or mitigated. A complete safety assessment considers not only those personnel who are directly involved in a hydrogen process, but also those who may not be involved in the process at all, but are still at risk due to these hazards.
- **Equipment.** Damage to or loss of equipment or facilities must be prevented. Damage to equipment can be both the cause of incidents and the result of incidents. An equipment failure can result in collateral damage to nearby equipment and property, which can trigger additional equipment failures or even present additional risks. A complete safety plan must consider and minimize serious risk of equipment and

property damage.

- **Business Interruption.** The prevention of business interruption, in addition to property damage, is important for commercial entities. Hazardous events may lead to interruption in providing service or product. This interruption is frequently expressed in terms of elapsed time before resumption of service or manufacturing. This time element can also be converted into dollars as a loss of revenue, or value added. A complete safety plan in those instances would include time element interruption, and where critical, include a contingency plan for providing needed services or manufacturing.
- **Environment.** Damage to the environment must be prevented. Any aspect of a natural or built environment that can be harmed due to a failure should be identified and analyzed. A qualification of the failure modes resulting in environmental damage must be included in the safety plan.

2. Required Safety Plans

Except for those relating to non-experimental computational or analytical work, all proposals for hydrogen-related solicitations must include a preliminary safety plan or summary, and funded projects must complete a more detailed safety plan before experiments/operations commence and must keep that plan current as part of the project. Safety plans should cover the work of any subcontractors and other collaborators. Individual solicitations may provide further direction regarding safety planning and requirements.

For R&D proposals, a safety plan will not be required until after the contract is awarded. However, R&D proposals involving the use of hydrogen should briefly describe the process to be used for evaluating, reviewing, and implementing a safety plan as part of the proposed R&D work (1-3 pages). This process description should clearly indicate the participation of all collaborating research groups and appropriate personnel (safety engineers, researchers, students, postdocs, etc.).

The table below summarizes safety plan requirements:

Type of Project	For Proposals	For Projects
Computational/Analytical	None	None
Research and Development (R&D)	Summary safety plan required (1-3 pages)	Safety plan required
Technology Validation and Demonstration (TV&D)	Preliminary safety plan required	Safety plan required

3. Preliminary Safety Plans

For Technology Validation and Demonstration project proposals, the preliminary safety plan needs to include the use of methodologies for identifying and analyzing safety risks, for mitigating these risks, and for communicating safety events to the necessary parties. The following items must be included in the preliminary safety plan.

3.1 Identification of Safety Vulnerabilities (ISV)

A. The formal means by which potential safety issues on major process steps, operations and facilities will be identified should be outlined. There are several

options for how this identification and analysis may be accomplished. The following options are suggested, but similar methods and analytical techniques may be used as well.

1. Preliminary Failure Modes and Effects Analysis (FMEA)
2. "What-if" analysis
3. Comprehensive identification and classification hazard analysis
4. Hazard and operability analysis (HAZOP)
5. Checklist analysis
6. Fault tree analysis
7. Event tree analysis
8. Probabilistic Risk Assessment (PRA)
9. Appropriate equivalent methodology

These ISV methodologies and analysis tools are further discussed in Section 4.1 Identification of Safety Vulnerabilities (see Page 5).

B. In addition to the preliminary ISV evaluation, a plan for preparing the final analysis or assessment that identifies significant safety concerns should be included. Published data on potential failures, rates of failure and means of mitigation should be used when available. If data are not available, best engineering practices may be used.

3.2 Outline of the Risk Mitigation Plan that will apply to the project based on the preliminary ISV. The Risk Mitigation plan should include the following:

A. **Description of how safety performance will be measured and monitored** to ensure that the ISV is updated regularly as data become available. The description should discuss how changes affecting safety will be screened and implemented including written procedures to manage changes to chemicals and other materials, technology, equipment, and procedures; and any changes to the facilities that affect the operation. The Management of Change (MOC) procedures should ensure that the following considerations are addressed prior to any change:

- The technical basis for the proposed change,
- Impact of change on safety and health,
- Modifications to operating procedures,
- Necessary time period for the change and
- Authorization requirements for the proposed change.

B. **Description of method to establish and maintain safety documentation.** This information should pertain to the process technology as well as equipment, chemicals and other materials being used in the process. It should include how maintenance records will be collected and/or automated and what data on

reliability (e.g., damage mechanism, mean time between failures, failure effect, etc.) will be obtained.

C. **Description of Standard Operating Procedures.** The proposal should outline the steps that have been and will be taken to develop and maintain Standard Operating Procedures (SOP). SOPs should be developed, documented, and implemented for each process with the active involvement of project personnel. These SOPs should provide clear instructions for conducting processes in a safe manner. They should include:

- Steps for each operating phase,
- Operating limits,
- Safety considerations,
- Safety systems and their functions and
- Emergency shut-down.

SOPs should be readily accessible to personnel involved with the process, and be updated regularly to reflect any changes to chemicals and other materials, equipment, technologies, and facilities.

D. **Description of Employee Training.** The proposal should include a description of how safety training will be administered to all employees working on the project. Training encompasses initial training, training on changes, and refresher training. A means for two-way communication should be established to enable personnel to communicate their safety concerns. A discussion of how training will be documented should be included.

E. **Description of Procedures to Ensure Equipment Integrity.** The proposal should outline the procedures by which the integrity of project equipment will be assured at initial commissioning and through on-going maintenance, inspection and testing. The plan should identify how and when any identified deficiencies are to be corrected.

F. **Emergency Response Plan.** The proposal should outline provisions for the emergency response plan for the facility, neighboring occupancies and/or the public at-large, as applicable.

3.3 Outline for the Communications Plan that the project manager will develop and implement during the project. This plan should include a description of:

A. Safety reviews to be conducted during the design, development and operations phases of the project and how they will be reported to DOE and to other pertinent organizations, and
B. The investigation and reporting process for each incident which resulted in, or could reasonably have resulted in, an unintended release of hydrogen or injury to people, equipment or the environment.

4. Safety Plan Preparation

Project safety plans need to include the use of methodologies for identifying and analyzing safety risks dealing with major process steps, operations and facilities, for mitigating these risks, and for communicating safety events to the necessary parties.

Safety assessments performed as part of developing a safety plan can take a number of approaches. One approach is noted here:

1. Perform safety assessment before construction begins—during design phase. Maintain construction oversight throughout the project.

2. Review system design against pertinent existing codes and standards (ASME, NFPA, etc.) and/or best engineering practices.

3. List hazards and safety issues not covered adequately in existing codes and standards. Which of these additional hazards and safety issues are of greatest concern to this particular project? Explain the basis for prioritization.

4. Develop detailed, reasonable-worst-case, credible scenarios describing process upsets, human errors, system failures, etc. that could result in unwanted or unacceptable consequences from the hazards and issues identified in Steps 2 and 3. These scenarios can be postulated without regard to existing design safety features. For each scenario, the impact to personnel, equipment, business interruption or environment should be assessed both with and without credit for existing active mitigation systems (systems that require mechanical, human, or electrical actuation or intervention.)

5. Identify and correct construction and code problems and deviations

    a. Identify and brief appropriate permit regulatory, and safety personnel early in the project (site/location specific).
    b. Address mechanical and/or electrical issues, storage separation distances, component ratings, ventilation, etc.
    c. Identify “new” hazards, if any—some hazards are equivalent to other commonly accepted public and industrial hazards
    d. Hazards can be characterized in terms of form, quantity, and location.

General guidance, requirements and examples for preparing the safety plan are covered below.

4.1 Identification of Safety Vulnerabilities

As previously stated, the Identification of Safety Vulnerabilities (ISV) can be in the form of any one or more of several different methodologies as chosen by the project team. This demonstrates that they have assessed and integrated safety into the proposed project at the earliest stages. The methodologies are all established industry practices for safety

and/or reliability engineering. The purpose is to analyze design components and system-level interactions for safety hazards and to demonstrate an understanding and anticipation of component failures. The most important objective is the prevention of problems before they occur. In the case of a failure, the ISV will lead to minimizing the effects of that failure. In a sense, it is a reliability tool as well as a safety tool, as it can help to identify areas within a system that are prone to failure.

Prior to performing the ISV, efforts should be made to compile information central to the system. Pertinent information includes:

- component specifications and configurations,
- component interaction information,
- operating procedures and
- equipment types and location (indoors, outdoors, laboratory hood, etc.).

Information available from earlier projects may be effective in the collection of the above information.

The following sections provide descriptions and examples for various ISV methodologies.

FMEA

Various methodologies exist for the performance of a FMEA, and numerous FMEA guides are available from traditional industry sources. Guidelines on general safety information are available in various government and military documents, including MIL-STD-882C and MILSTD-1629A. In addition, websites such as **http://www.fmeainfocentre.com/** (a non-commercial web-based inventory dedicated to the promotion of Failure Mode and Effect Analysis) and the NASA Technical and Information Program's **http://www.sti.nasa.gov/new/fmea33.html** may provide additional information on the development of FMEAs.

In general, the FMEA process follows a standard procedure, as detailed below:

1. Identify top level hazards/events
2. Identify related equipment/components/processes
3. Identify potential failure modes and effects
4. Identify design inherent safety
5. Identify potential prevention and/or mitigation corrective actions

This outline is repeated for every component of every system. System-level failures must be included as well, as there are cases where every component may work well individually, but the system still fails.

A FMEA can be performed via two different approaches. The hardware, or component, analysis is the identification and analysis of ramifications of component failures. This method is a bottoms-up approach, wherein failures are initiated on the subsystem level.

The functional approach is a top-down method, starting at the system level. This is more suitable when specific components have not yet been chosen. Either approach is acceptable; both may be best in some cases. The development of the FMEA is a continuous process, and the document should evolve as the system design changes. A discussion and worked example of a FMEA can be found in *Guidelines for Hazard Evaluation Procedures*, a publication of the American Institute of Chemical Engineers (Ref 1).

"What If" Analysis

The methodology behind a "What If" analysis is a speculative process where questions of the form "What if … (hardware, software, instrumentation, or operators) (fail, breach, break, loose functionality, reverse, etc.)..?" are formulated and reviewed. The method has as its basic features:

1. the scope definition,
2. the team selection,
3. the review of documentation,
4. facilitated question and response evaluation with consequences, (which includes the likelihood rating, the release-severity rating, and the risk-based assessment classification) and
5. summary tabulation to the set of questions.

The "What If" questions are facilitated during a team review of segmented sections of equipment found in an engineering drawing (such as the piping and instrumentation diagram, P&ID) and/or for each step in an operating procedure. The team review usually focuses on each individual segment as the basis to ask and respond to questions as a group. Questions are formulated in the style of the question, "What if .... ?" The questions should address the following types of actions:

- Equipment failure,
- process condition upsets due to temperature, pressure, or feed upsets,
- instrumentation failure,
- interfacing utility failures,
- operator timing, out-of-order sequencing, endpoint failures, or inattentive departures from operating procedures during normal operations,
- start-up or shutdown maintenance related accidents
- site related events, such as handling related accidents,
- third party events such as accidents or storms.

A good example of a "What If" analysis can be found in Ref 1.

Hazards Analysis - WSMS Comprehensive Approach

In 1998, Westinghouse Safety Management Solutions (WSMS) developed a comprehensive hazards identification and classification process that uses a graded approach to assessing hazards (Ref 2). The system is based on a DOE process for establishing and documenting operational safety for its nuclear and chemical process

facilities. The WSMS process was applied at the time to a safety assessment of hydrogen-fueled mining equipment.

The WSMS approach starts with hazard identification, that is, a listing of all hazardous materials or energy sources associated with the project. These sources are characterized as to location, form, and quantity. The second step in the analysis is the development of detailed reasonable-worst-case, credible scenarios describing process upsets, spills/leaks, system failures, human errors, etc. Each scenario is then placed in a "Risk Bin," a matrix where likelihood of occurrence is assessed together with the consequence of occurrence. The combination of likelihood and consequence results in an assignment of a graded level of risk.

An example of this type of comprehensive hazard analysis showing an identification table and the results of a sample evaluation is shown in Appendix A from Ref 2.

HAZOP

The Hazard and Operability Analysis (HAZOP) was originally developed to identify both hazards and operability problems at chemical process plants, particularly for processes using new technologies under development. The technique is also useful for analyzing the failure implications for existing processes as well.

A HAZOP requires an interdisciplinary team and an experienced team leader. The purpose of a HAZOP is to review a process or operation systematically to identify whether process deviations could lead to undesirable consequences. Reference 1 states that the technique can be used for continuous or batch processes and can be adapted to evaluate written procedures. It can be used at any stage in the life of a process. HAZOPs usually require a series of meetings in which the team systematically evaluates the impact of deviations using process drawings. The team leader uses a fixed set of guide words and applies them to process parameters at each point in the process. Guide words include "No," "More," "Less," "Part of," "As well as," "Reverse," and "Other than." Process parameters considered include flow, pressure, temperature, level, composition, pH, frequency, and voltage. As the team applies the guide words to each process step, they record each deviation with potential causes, consequences, existing or potential process safeguards and actions needed to prevent or mitigate the consequences, and/or the need for additional analysis to evaluate the impacts of the deviation or design the safeguards.

HAZOPs require more resources than simpler techniques such as FMEA. Ref 1 contains an extensive description and worked example of the HAZOP procedure.

Checklist Analysis

A checklist analysis is simply just that – it evaluates the process in question against existing guidelines using a series of checklists. This technique is most often used to evaluate a specific design, equipment or process for which an organization has a significant amount of experience. If a new project, for instance, is being performed using an existing system, checklists that cover accident prevention or best practices may already be in place for the existing system. This would make a checklist analysis on the new project easy to perform. If no appropriate checklist(s) exists, a range of project personnel of different backgrounds can develop it.

In general, once the system to be analyzed and its boundaries are defined, it is divided into subsystems or smaller, as appropriate. Then existing checklists are gathered for the various subsystems, and those that don't exist are developed. The questions put forth in the checklist are answered and, where needed, acted upon.

Ref 1 and 3 give specific examples of the use of Checklist Analysis.

Fault Tree Analysis

Fault Tree Analysis is a deductive (top-down) method used for identification and analysis of conditions and factors that can result in the occurrence of a specific failure or undesirable event. The strength of the fault tree model is that it addresses multiple failures, events, and conditions. The analysis proceeds by constructing a graphical model of failure using a set of standardized logic symbols to represent the relationship of faults (failures, conditions, events) with the potential to result in the occurrence of the specific failure condition being analyzed. Fault tree analysis can address:

1. Independent, dependent, simultaneous, and common mode failures in systems and/or processes.
2. Effects of human errors, including operator and maintenance errors and external conditions.

The level of detail addressed in a fault tree is generally determined by the amount of data available, the desired level of resolution of the model, and the use of the fault tree (e.g., part of a larger study or not). Fault trees are generally developed and evaluated using available software packages which can produce the fault tree diagram, lists of contributing events, and evaluate the likelihood of occurrence of the top event and contributing events.

Ref 1 discusses this option and also presents good examples of Fault Tree Analysis.

Event Tree Analysis

Event tree analysis is an inductive approach used to identify and quantify a set of possible outcomes. The analysis starts with an initiating event or initial condition and includes the identification of a set of success and failure events that are combined to produce various outcomes. The goal of an event tree analysis is to identify the spectrum and severity of possible outcomes and determine their likelihood. Event tree analysis produces a graphical representation of sequences of events leading to various outcomes.

An event tree analysis of an initial (initiating) event which must have successful safety system response to prevent an undesired end state, starts with the identification of all the safety systems that must function to prevent or mitigate undesired consequences. Then the systems are listed in order of expected operation and the success or failure of each system is then postulated. The effect of these successes or failures are identified and combined as individual sequences of events, sometimes referred to as accident sequences or scenarios. The result is a set of sequences representing combinations of failures and

successes with varying consequences ranging from successful response to the maximum possible damage. Based on experience data and failure analysis of the events in each sequence, the likelihood of each sequence is determined. Event trees are generally developed and evaluated using available software packages which can produce the event tree diagram, evaluate the likelihood of occurrence of each sequence, and group the sequences into groups of similar outcomes.

Ref 1 discusses this option and also presents good examples of Event Tree Analysis.

Probabilistic Risk Assessment

A Probabilistic Risk Assessment (PRA) is an organized process for answering the following three questions:

1. What can go wrong?
2. How likely is it to happen?
3. What are the consequences?

PRA methodology originated in the nuclear power and aerospace industries and has been adapted for use in the chemical industry, where this approach is called "Chemical Process Quantitative Risk Analysis" or CPQRA. A variety of analytical techniques are used in the performance of a CPQRA, depending on the scope and complexity of the problem to be addressed. The analysis steps and methods involved in performing a CPQRA are as follows.

1. Problem definition. Identification of study goals, choice of the risk measures to be used, selection of the depth of study to be performed, identification of the information resources required to perform the study.
2. System description. Compilation of the process/plant information (i.e. site location, weather data, process flow diagrams, piping and instrumentation diagrams, etc.) needed to perform the analysis.
3. Hazard identification. A critical step in CPQRA. Identifies the potential energy sources that can affect the system being analyzed and the potential hazardous material that can be released. Depending on the problem, approaches to be used to identify hazards include; a) data analysis, b) hazard identification check list, c) what-if analysis, d) hazard analysis techniques, e.g., HAZOP, FEMA, or PHA (Preliminary Hazard Analysis).
4. Incident enumeration and selection. Starts with an initial identification of all possible incidents without regard for importance or initiating event using processes such as data assessment or FMEA. Incidents are grouped by type and the most significant incidents from each type are determined and used to represent all identified incidents for the purpose of further analysis.
5. CPQRA model construction. Appropriate likelihood models and consequence models are selected and integrated into an overall model to produce and present risk estimates for the system under study. Likelihood models include use of historical data on events, fault trees, and/or event trees. Consequence analysis

tools include fire, explosion, and direct (burns, impacts, etc.), health effects (lethal dose, long-term consequences) and material dispersion models.

6. Likelihood estimation. The methodology used to estimate the frequency or probability of the occurrence of an event or component failure can be obtained from historical data, or from developing and quantifying failure sequence models using fault tree and event tree analysis methods.
7. Consequence estimation. The methodology used to determine the potential for damage or injury from specific incidents includes direct (burns, impacts, etc.) and health effects (lethal dose, long-term consequences) models.
8. Risk estimation. The process of combining the consequences and likelihoods of all potential incidents to provide a measure of risk. The risks of all selected incidents are individually estimated and combined to give an overall measure of risk using techniques such as the development and quantification of damage states and plotting the risk in a graphical form (e.g. cumulative complementary distribution functions).
9. Utilization of risk estimates. Results from a risk analysis are used to make decisions based on the significance of events, failures, and/or conditions to the overall risk estimates.

Ref 4 provides a detailed description of the Chemical Process Quantitative Risk Analysis approaches and methodologies.

4.2 Risk Mitigation Plan

The purpose of a risk mitigation plan is to minimize the greatest risks. It is essentially an extension of the ISV analysis, as its construction usually follows that development. After identifying safety vulnerabilities, the project team will have a prioritized list of safety aspects that require action. A risk mitigation plan provides detailed design and operational modifications for each issue on that list. Typical aspects of a risk mitigation plan include a discussion of mitigation measures, a cost effectiveness analysis, and an implementation strategy.

Mitigation plans are expected for events that could reasonably result in an unintended release of hazardous material or in injury to people. A risk mitigation plan assesses the scenarios and identified hazards from the safety assessment. The plan should determine the likelihood of occurrence, which could be expressed in frequency of occurrence, and the severity of consequence. It should consider the cause(s) of the scenario (or initiating event[s]) and the hazardous material or energy released as a result of the scenario. During this phase of the analysis, focus should be on those hazards that are of greatest concern.

Risk binning is one analysis tool for risk mitigation. Each hazard can be plotted on a frequency/consequence (risk) matrix, which would indicate its level of risk – high, moderate, low, or negligible. For example, if a potential hazard's frequency is unlikely, and its consequence level is high, it would be a high risk. If a risk binning tool is used, the criteria for assigning frequency and consequence categories should be included. The uncertainty of assigning events to these bin categories should also be addressed. Risk

binning can consider a base case design with any provided prevention and mitigation devices to determine if additional facilities are warranted. The following categories could be used for organizing and analyzing data:

- Event number
- Event category
- Postulated event description
- Causes
- Preventive features
- Frequency level
- Mitigative features
- Consequences
- Risk bin number

The consequences category should always include damage to a structure due to overpressure, or a secondary fire where the hydrogen leak is ignited. Consideration should also be given to the risk of an equipment/facility fire started elsewhere that endangers facilities and personnel where hydrogen is being used.

An example of a risk-binning matrix and frequency and consequence criteria tables are shown in Appendix B.

As already mentioned, risk mitigation also includes safety performance monitoring, management of change, safety documentation collection and maintenance, standard operating procedures development and use, employee training, and equipment maintenance. Although descriptions of these have already been given, some additional information is warranted for some of these items, and this material follows.

Safety Performance Measurement and Management of Change Reviews

A good measure of a safe hydrogen project is its insurability, and an important step is to quantify risks. A thorough safety plan will serve as a basis on which the risks associated with a technology may be measured. The plan needs to include a description of how safety performance will be measured and monitored, while ensuring that the ISV analysis is updated regularly as operating data becomes available.

The method to be used for reviewing the safety implications of any potential changes to project materials, processes, equipment, and operating/repair procedures should be stated along with a management commitment to implement the MOC procedure (see 3.2A). In addition, the contractor should establish and implement written procedures to manage changes (except for “replacements in kind”) to process chemicals, technology, equipment, and procedures

Employee Training

It is crucial to provide hydrogen safety training for all project personnel responsible for handling equipment containing hydrogen. The training program/procedures should be described and a management commitment to implement the procedure should be documented. An employee training program might have steps similar to these:

1. Each employee presently involved in operating a process, and each employee before being involved in operating a newly assigned process, is trained in an overview of the process and in the operating procedures. The training includes emphasis on the specific safety and health hazards, emergency operations including shutdown, and safe work practices applicable to the employee's job tasks.
2. In lieu of initial training for those employees already involved in operating a process, the contractor certifies in writing that the employee has the required knowledge, skills, and abilities to safely carry out the duties and responsibilities as specified in the operating procedures.
3. Refresher training is provided to each employee involved in operating a process to assure that the employee understands and adheres to the current operating procedures of the process. The contractor, in consultation with the employees involved in operating the process, determines the appropriate frequency of refresher training.
4. Training documentation: The contractor ascertains that each employee involved in operating a process has received and understood the training. The contractor keeps a record which contains the identity of the employee, the date of training, and the means used to verify that the employee understood the training.

Procedures to Ensure Equipment Integrity

Equipment integrity maintenance might take a form similar to the following:

1. The contractor/project team establishes and implements written procedures to maintain the on-going integrity of process equipment, including calibration procedures for safety-related equipment.
2. The contractor trains each employee involved in maintaining process equipment to ensure that the employee can perform the job tasks in a safe manner. An overview of the process and its hazards and the operating procedures applicable to the employee's job tasks are provided.
3. The frequency of inspections and tests of process equipment is consistent with applicable manufacturers' recommendations and best engineering practices, and more frequently if determined to be necessary by prior operating experience.
4. The contractor documents each calibration, inspection and test, including any hydrotests or leak tests, performed on process equipment. The documentation identifies the date of the inspection or test, the name of the person who performed the inspection or test, the serial number or other identifier of the equipment on which the inspection or test was performed, a description of the inspection or test performed, and the results of the inspection or test.

4.3 Communications Plan

The communications plan is a description of reports that are made when an incident occurs. A reportable incident is broadly defined as a failure that results in damage to any of the factors (personnel, equipment, and environment) discussed above or any unintentional hydrogen release. The magnitude of these risks can vary widely, and some

discretion is left to the investigator. However, certain incidents are reportable under any conditions. These failures are as follows:

- Any failure that results in an injury or lost time accident
- Any failure that results in down time to process equipment
- Any unintentional hydrogen release that ignites or is sufficient to sustain a flame, if ignited

This list is not inclusive of all reportable incidents, but is indicative of the severity of incidents that must be reported.

5. References

1. *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples,* Center for Chemical Process Safety, American Institute of Chemical Engineers, 1992.

2. *Preliminary Safety Evaluation for Hydrogen-fueled Underground Mining Equipment*, DA. Coutts and J.K. Thomas, Westinghouse Safety Management Solutions, Aiken, SC, Publication WSRC-TR-98-00331, September 1998. (This reference includes information from *Preparation Guide for US Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports,* DOE-STD-3009-94, July 1994.)

3. Risk-based decision-making guidelines, United States Coast Guard http://www.uscg.mil/hq/g-m/risk/e-guidelines/RBDM/html/vol3/02/v3-02-cont.htm

4. *Guidelines for Chemical Process Quantitative Risk Analysis*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 2000.

Appendix A – Example Hazard Identification Table

Table 1-1.--HAZARD ENERGY SOURCES, MATERIALS AND EQUIPMENT

Hazard Energy Sources and Materials

Location (identifier for system, sub-system, or operational feature in this facility section)	Electrical																		Thermal								Friction							
	Battery Banks (BB)	Cable Runs (CB)	Diesel Units (DU)	Electrical Equipment (EE)	Hot Plates (HP)	Heaters (HT)	High Voltage (HV,>220 v)	Locomotive, Electrical (LE)	Motors (MT)	Pumps (PM)	Power Tools (PT)	Switchgear (SG)	Service Outlets, fittings (SO)	Transformers (TF)	Transmission Lines (TL)	Underground Wiring (UW)	Wiring (WR)	Other	Bunsen Burner, Hot Plates (BR)	Electrical Equipment (EE)	Furnaces (FR)	Heaters (HT)	Steam Lines (SL)	Welding Torch (WT)	Exothermic Reactions (ER)	Other	Belts (BL)	Bearings (BR)	Fans (FN)	Gears (GE)	Motors (MT)	Power Tools (PT)	Other
Working vehicle	X	-	-	X	X	-	1	X	X	X	X	-	X	X	2	-	X	3	-	X	-	-	-	X	4	5	X	X	X	X	X	X	X
Underground refueling operation	X	-	-	X	X	-	1	X	X	X	X	-	X	X	2	-	X	3	-	X	-	-	-	X	X	5	X	X	X	X	X	X	X
Refueling transport vehicle	X	-	-	X	X	-	1	X	X	X	X	-	X	X	2	-	X	3	-	X	-	-	-	X	4	5	X	X	X	X	X	X	X
Fuel transfer (not covered)																																	
Hydrogen mfg. (not covered)																																	

Hazard Energy Sources and Materials

Location (identifier for system, sub-system, or operational feature in this facility section)							Open Flame					Flammables				Explosives				Potential					Kinetic								
	Pyrophoric (Pu & U Metal (PU)	Pyrophoric (Other)	SC (Nitric Acid and Organics) (HN)	SC (Other)	Combustible Materials (CB)	Uncontrolled Chem. Reactions (CH)	Bunsen Burners (BR)	Torches (WT)	Pilot Lights (PL)	Gas Welding (GW)	Other	Flammable Gases (FG)	Flammable Liquids (FL)	Flammable Mixtures (FA)	Other	Explosive Gases (EG)	Hydrogen/Tritium (HZ)	Propane (PP)	Explosive Chemicals (EC)	Other	Gas Bottles (GB)	Gas Receivers (GR)	Pressure Vessels (PV)	Steam Headers/Lines (ST)	Other	Fans (FN)	Pumps (PM)	Motors (MT)	Rotating Machinery (RO)	Other	Non-Facility Event (Explosion) (EX)	Non-Facility Event (Fire) (FT)	Non-Facility Event (Other) (OT)
Working vehicle	-	6	-	-	7	-	-	X	-	X	-	X	-	X	8	X	X	-	-	9	X	-	X	-	X	X	X	X	X	X	-	-	10
Underground refueling operation	-	6	-	-	7	-	-	X	-	X	-	X	-	X	8	X	X	-	-	9	X	-	X	-	X	X	X	X	X	X	-	-	10
Refueling transport vehicle	-	6	-	-	7	-	-	X	-	X	-	X	-	X	8	X	X	-	-	9	X	-	X	-	X	X	X	X	X	X	-	-	10
Fuel transfer (not covered)																																	
Hydrogen mfg. (not covered)																																	

Hazard Energy Sources and Materials

Hazard Energy Sources and Materials

Location (identifier for system, sub-system, or operational feature in this facility section)				Ionizing Rad.					Hazardous Materials								Natural Phenomena									Vehicles in Motion						
	Radiological Material (RM)	Fissile Material (FM)	Non-Ionizing Radiation (NI)	Fissile Material (FM)	Radiography Equipment (RE)	Radioactive Materials (RM)	Radioactive Sources (RS)	Other	Alkali Metals (AM)	Asphyxiants (AS)	Biological (BI)	Carcinogens (CA)	Oxidizers (OX)	Corrosives (CO)	Toxics (TX)	Other	Earthquake (EQ)	Flood (FD)	Lightning (LT)	Rain (RN)	Snow, Ice (SN)	Freezing Weather (FW)	Straight Wind (SW)	Tornado (TO)	Other	Airplane (AP)	Helicopter (HL)	Train (TN)	Truck/Car (TR)	Forklift/ Lift Truck (FK)	Other	Crane/Hoist (CR)
Working vehicle	-	-	X	-	-	-	X	-	-	11	-	X	X	12	-	13	X	14	15	X	X	X	X	X	16	-	-	X	X	X	17	X
Underground refueling operation	-	-	X	-	-	-	X	-	-	11	-	X	X	12	-	13	X	14	15	-	-	-	-	-	16	-	-	X	X	X	17	X
Refueling transport vehicle	-	-	X	-	-	-	X	-	-	11	-	X	X	12	-	13	X	14	15	X	X	X	X	X	16	-	-	X	X	X	17	X
Fuel transfer (not covered)																																	
Hydrogen mfg. (not covered)																																	

An X refers to the hazards considered applicable.
A number indicated an applicable hazard with an explanation at the end of this Appendix.

Source: Ref 2

Notes

1. High Voltage (HV)
Voltages above 1000 volts are typically not permitted in the underground environment. (There are exceptions for transmission lines. See the discussion below.) Thus, when the vehicles are underground, there is not exposure to these voltages. If the vehicles exit the mine, there is potential for overhead transmission lines that carry these voltages.

2. Transmission Lines (TL)
There are instances where 4160 or 7200 volt transmission lines have been installed in mines. These insulated conductors have very limited protection from vehicle impact.

3. Other
Within the mine there is the potential for exposed conductors, which would be used to support trolley lines. Typically these systems range from 300 to 600 volts DC.

4. Exothermic Reactions (ER)
The hydrogen-oxygen reaction in the fuel cell is an exothermic reaction

5. Other
Brake disks on mining equipment can get hot and have been known to cause fires.

6. Pyrophoric (Other)
The metal hydride is slightly flammable.
Coal under some conditions can be pyrophoric.

7. Other
Combustible liquids (flashpoint above 100°F) are present. These can include hydraulic fluids and diesel fuel. The diesel fuel might be contained in transport piping where vehicles are being driven.
Coal, coal dust and conveyor belts are all present.

8. Other
Working vehicles might transport explosives.

9. Other
Pressurized air (~150 psi) and water (~250 psi) are common.
For vertical shaft or sloped entries there can be considerable potential energy. In addition vehicles can rollover on uneven terrain.

10. Non-Facility Event (Other) (OT)
Surface muting near an underground mine can cause a roof collapse.

11. Asphyxiants (AS)
Black damp has occurred in some mines. This term describes a scenario where an opening is made between an abandoned mine, which is oxygen deficient, and a working mine. The oxygen level in the working mine can quickly drop to untenable levels. Methane is an asphyxiant.

12. Corrosives (CO)
Batteries on the hydrogen-fueled vehicles and nearby vehicles contain acid.

13. Other
There are several materials (e.g., polyurethane) which are used to seal air dams. Hydrocarbons can leak from walls and the roof of some mines.

14. Flood (FD)
Rapid flooding can occur. Both the rising water and the water flow can cause problems. Water can also collect in low spots where vehicles will need to drive through.

15. Lightning (LT)
Both inside and outside the mine.

16. Other
Roof collapse can range from localized rock falls, which do not damage most vehicles, to extensive collapses.
Bumps are phenomena where the floor will rise or walls will move. It can occur rapidly with no indication. This movement can collapse tunnels crushing the vehicle and its occupants.

17. Other
Other equipment that can be present (e.g., scoops, load haul dumps, roof bolters). Most of these will be characterized as very heavy, difficult to maneuver and with limited operator visibility.

Table 2-1.--Hazard evaluation results

Event		Postulated event	Causes	Preventive features		Freq.	Method of	Mitigative features		Consequence level[1]		Risk
no.	type	description		design	admin.	level[2]	detection	design	admin.	people	property	bin #
1	E-1	Fire starts remote from vehicle and propagates to involve the hydrogen system. Hydrogen is released.	General fire hazards		Fire protection program	U[3]	Visual, smell	Mine arrangement	Emergency team	H[4]	H	4
2	E-1	Fire starts on vehicle, but not in hydrogen system. Hydrogen is released.	Hot brakes, electrical short	Fuses	Brake maintenance		Visual, smell	Vehicle design, suppression system	Emergency team	H	H	4
3	E-1	Fire starts in hydrogen components. Hydrogen is released	Hydrogen leak		Fire protection program	U	Visual, smell	Hydrogen system integrity	Emergency team	H	H	4
4	E-1	Coal dust ignition by vehicle electrical system. Hydrogen is released	Electrical contacts close	Classified equipment	Inspections	EU	Visual, heat	Mine arrangement	Coal dusting	H	H	7
5	E-2	Battery explosion damages hydrogen system causing leak.	Battery short	Design		U	Visual, equipment fails to run	Design		H	H	
6	E-2	Fire starts remote from vehicle and involves hydrogen system. Hydride tank bursts.	General fire hazards	Relief protection	Fire protection program	EU[5]	Visual, smell	Mine design	Emergency team	H	H	7
7	E-29	Fire starts on vehicle, but not in hydrogen system. Hydride tank bursts.	General fire hazards	Relief protection	Fire protection program	EU	Visual, smell	Vehicle design, suppression system	Emergency team	H	H	7

Table 2-1.--Hazard evaluation results

Event no.		Postulated event description	Causes	Preventive features: design	Preventive features: admin.	Freq. level[5]	Method of detection	Mitigative features: design ,	Mitigative features: admin.	Consequence level': people	Consequence level': property	Risk bin #
8	E-2	Fire starts in hydrogen components. Hydride tank bursts.	Hydrogen leak	Relief protection	Fire protection program	EU	Visual, smell	Hydrogen system integrity	Emergency team	H	H	7
9	E-2	Hydrogen explosion	Delayed ignition after leak	Design of vehicle, ventilation		U	Visual	Hydride metal	Emergency team	H	H	7
10	E-2	Methane explosion	Methane release with ignition	Ventilation		A[6]	Meters	Mine layout		H	H	1
11	E-2	Coal dust explosion	Methane or hydrogen explosion	Ventilation	Coal dusting	EU	Visual, sound	Mine layout		H	H	7
12	E-2	Explosives damage vehicle and release hydrogen	Inadvertent explosion during transport	Packaging		EU	Visual, sound	Hydride metal		H	H	7
13	E-3	Battery leaks acid onto hydrogen system and causes a hydrogen leak.	Battery damage	Design	Vehicle maintenance	EU	Visual		Vehicle inspections	H	H	7
14	E-3	Hydride tanks leak " contents and causes fire	Tank punctured	Design		EU	Visual, smell	Hydride metal selection		H		7
15	E-4	Fuelcell shorts	Damage to membrane	Design		U	Vehicle fails to run			N	L[7]	6
16	E-4	Fuelcell membrane fails and a small deflagration occurs.	Membrane defect	Design		U	Vehicle fails to run			N	L	6
17	E-4	Coal dust enters and damages fuelcell	Filter left off	Design	Training	U	Vehicle fails to run			N	L	6

Table 2-I.--Hazard evaluation results

Event no.	Event type	Postulated event description	Causes	Preventive features: design	Preventive features: admin.	Freq. level[2]	Method of detection	Mitigative features: design	Mitigative features: admin.	Consequence level': people	Consequence level': property	Risk bin #
18	E-4	Transmission line falls on equipment and damages hydrogen system containment.	Electrical arching		Inspection of transmission lines	EU	Visual	All hydrogen components protected from direct contact	Keep maintenance access doors on vehicle closed.	H	H	7
19	E-4	Hydrogen system damaged by welding on vehicle	Inattentive welder		Control of welding activities	EU	Visual			H	H	7
20	E-4	Shrapnel damages hydrogen system	Accumulator ruptures, drive shaft breaks	Design	Vehicle maintenance	EU	Visual, sound	Hydride metal selection		H	II	7
21	E-4	Shrapnel damages fuel cell and fire occurs	Accumulator ruptures, drive shaft breaks	Design	Vehicle maintenance	EU	Visual, sound	Hydride metal selection		H	H	7
22	E-4	Major damage to hydrogen system containment	System dropped during vertical transit			EU	Visual	Hydride metal selection		H	II	7
23	E-4	Vehicle impact damages hydrogen containment	Vehicle to vehicle, vehicle to wall		Training	A	Visual	Vehicle design		H	H	
24	E-5	Black damp	Open entry to old workings	Shut-off timer	Work planning	U	Visual, low oxygen, high methane content			H	M	4
25	E-5	Acid damage to hydrogen system	Exposure to high acid water	Material selection	Control pH of water	U	Visual		Inspections	H	H	4

Table 2-1.--Hazard evaluation results

Event		Postulated event	Causes	Preventive features		Freq.	Method of	Mitigative features		Consequence level[1]		Risk
no.	type	description		design	admin.	level[2]	detection	design	admin.	people	property	bin #
26	E-6	Flooding	Water intrusion, pipe break		Work planning	U	Visual	Pumps		H	H	4
27	E-6	Roof collapse[5]		Roof bolting	Inspections	U	Visual	Vehicle design		H	H	4
28	E 6	Bump				EU[9]	Visual			H	H	7
29	E-7	Vehicle left in operation after evacuation	Fire, explosion, roof fall causes operator to leave	Shut-off timers		A	Operator interview			L	H	1
30	E-7	Vehicle operated in sub-2% methane	Methane leaks			A				N	L	3

[1] N, negligible; L, low; M, moderate; H, high

[2] A, anticipated; U, unlikely; EU, extremely unlikely; BEU, beyond extremely unlikely.

[3] The frequency that a severe fire would occur in a mine is judged to be unlikely. If it were anticipated, many mines would be experiencing severe fires. This is not the current situation for the mining industry.

[4] As discussed in Section 6.4, all events where hydrogen is released have the potential for an explosion. Thus, all events that might lead to a hydrogen release are classified as having a high consequence. This is the bounding consequence for a hydrogen explosion. Those events where ignition of the hydrogen does not occur would be expected to have a lower consequence.

[5] This frequency combines the frequency of a severe fire and the probability that the relief valve fails to operate.

[6] Small-scale explosions resulting from the ignition of small pockets of methane occur in many mines with no significant consequence. Many mines have experienced brief methane flashes at the working face with little or no consequences.

Damage to the membrane is considered to be more than a minor repair.

[8] This event captures all roof collapses. Consequences range from minor damage to equipment that does not require repair, to loss of entire passageway.

[9] The frequency of bumps is judged based on acceptable risk. If bumps are anticipated events, it is judged that the risk of personnel injury would be too high, and the mine would be closed. Thus, they must be unlikely or lower. When combined with the presence of a hydrogen-fueled vehicle the frequency is extremely unlikely.

Description of Columns in the Hazard Evaluation Results Tables

1. Event Number

Events are numbered to provide each with a sequential reference.

2. Event Category

Events were categorized according to the nature of the postulated release mechanism that directly initiates the postulated consequence. The categories are as follows:

- E-1 Fire
- E-2 Explosion
- E-3 Loss of Containment/Confinement
- E-4 Direct Hazard Exposure
- E-5 External Hazards
- E-6 Natural Phenomena
- E-7 Other

Events are categorized according to the event description rather than the event initiator. For example, a fire might be a postulated event that causes a tank to burst. This event would fall under category E-2 (Explosion) rather than E-1 (Fire), since the tank rupture is expected to result in a larger consequence than a fire without tank rupture.

3. Postulated Event Description

A brief description of a postulated event is given in this column of the Hazard Evaluation Tables. The event description clearly defines the nature of the event. It includes the type of event, its location, hazard source, affected system(s) or equipment, any interaction with other system(s), equipment, and/or hazards, and any pertinent operating characteristics.

4. Causes

A cause specifically states the failure, error, operational, and/or environmental condition that initiated the postulated event. The Hazard Identification Tables were used as a guide in developing specific causes for release events.

5. Preventive Features

A preventive feature is any feature that could readily be expected to act to prevent the event from occurring.

6. Frequency Level

Event frequency evaluation is a qualitative or quantitative process that involves assigning a frequency level to each event in the Hazard Evaluation Tables. The hazard analysis team determines which qualitative frequency level is appropriate for a particular event. This determination is based on the event's root cause(s) and may be either qualitative or

quantitative. The frequency level is recorded in the Hazard Evaluation Tables according to the definitions in Table 4.

7. Mitigative Features

Mitigative features are any features that are readily expected to act to reduce the consequences associated with the postulated event. Mitigative features are those which are assumed to be operable during an event or post event, and are not required to be operating prior to the event initiation. Therefore, mitigative features must be capable of withstanding the environment of the event. These might include engineered features (e.g. structures, systems, components, etc.), administrative controls (e.g. procedures, policies, programs, etc.), natural phenomena (e.g. ambient conditions, buoyancy, gravity, etc.), or inherent features (e.g. physical or chemical properties, location, elevation, etc.) operating individually or in combination.

8. Consequences

Event consequences are documented by specifying the potential for loss or damage based on the rankings established in Table 5.

9. Risk Bin Number

Using event frequency and consequence levels the hazard analysis team "bins" events in frequency-consequence space to assess relative risk based on Figure 4. The objective of risk binning is to focus attention on those events that pose the greatest risk to the specified receptors. Higher risk events are candidates for additional analysis.

Appendix B – Risk Binning Matrix: Frequency/Consequence Criteria

Frequency → / Consequence	Beyond extremely unlikely	Extremely unlikely	Unlikely	Anticipated
High	10	7	4	1
Moderate		8	5	2
Low		9	6	3
Negligible	11	12		

High risk

Low risk

Moderate risk

Negligible risk

Source: Ref 2

Frequency criteria used for risk-binning

Acronym	Description	Frequency level
A	Anticipated, Expected	> 1E-2/yr
U	Unlikely	1E – 4 < f ≤ 1E – 2/yr
EU	Extremely Unlikely	1E – 6 < f ≤ 1E – 4/yr
BEU	Beyond Extremely Unlikely	≤ 1E – 6/yr

Consequence criteria used for risk-binning

Consequence Level	Impact on Populace	Impact on Property/Operations
High (H)	Prompt fatalities Acute injuries – immediately life threatening Permanent disability	Damage > $50 million Production loss in excess of 1 week
Moderate (M)	Serious injuries Non-permanent disability Hospitalization required	$100,000 < damage ≤ $50 million Vehicle destroyed Critical equipment damaged Production loss less than 1 week
Low (L)	Minor injuries No hospitalization	Damage ≤ $100,000 Repairable damage to vehicle Significant operational down-time Minor impact on surroundings
Negligible (N)	Negligible injuries	Minor repairs to vehicle required Minimal operational down-time No impact on surroundings